U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MP
Phone: 202-267-0388
FAX: 202-267-4700

210199

USCG-2002-14069-4

COMDTPUB P16700.4
NVIC 10 02
OCT 21 2002

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 10 02

Subj: SECURITY GUIDELINES FOR VESSELS

Ref: (a) Navigation and Vessel Inspection Circular No. 4-02
(b) Title 33 CFR part 120 and 33 CFR part 128

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) establishes new guidelines for developing security plans, and implementing security measures and procedures. Under the authority in 50 U.S.C. 191 et seq., implemented at 33 C.F.R. Part 6, and reference (b), this circular covers all private and publicly operated vessels except as noted in paragraph 2.b. below.

2. ACTION.

   a. Captains of the Port (COTPs) are encouraged to bring this circular to the attention of marine interests within their respective zones of responsibility. This circular will distributed by electronic means only. It is available on the World Wide Web at **http://www.uscg.mil/hq/g-m/nvic/index.htm**.

   b. All vessel operators and owners are encouraged to consider the guidance provided in this Circular. This circular has been developed to assist vessel operators and owners to align with the security requirements being developed at the International Maritime Organization (IMO) and reflect good security practices for all vessels.

DISTRIBUTION – SDL No. 139

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		2	10		1			1						132	1			1								30
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

*NON-STANDARD DISTRIBUTION: B:a Commandant (G-MP/G-MOC/MO-1//MSE/MW/OPD/OPL/OPF-3) (1)

Therefore, U.S. vessels, including MODUs and public vessels, and foreign vessels calling at U.S. ports would benefit from initiating this guidance, which has been specifically developed for all vessels, except:

(1) Uninspected vessels other than towing vessels;
(2) Passenger vessels required to comply with reference (a) and (b);
(3) Ferries certified to carry more than 500 passengers and addressed by G-M letter 16611 dated 4 Sep 2002;
(4) Passenger vessels, other than offshore supply vessels as defined in 46 CFR 175.400, inspected under 46 CFR Subchapter T; and
(5) Vessels of War.

c. Fixed and floating platforms are not covered by this guidance. Separate guidance will be published for fixed and floating platforms.

d. Passenger vessels, unless exempted above, that are inspected under 46 CFR Subchapters H and K, barges, and towing vessels that comply with an industry standard that has been reviewed and accepted by the Coast Guard may be considered to meet this guidance.

e. These guidelines contain the suggested actions and procedures for facilities and vessels calling at marine facilities and are, by their nature, broadly crafted to cover all marine facility/vessel interfaces. The Coast Guard encourages representatives of marine facilities and vessels calling at them to jointly develop plans and actions going beyond these guidelines that will enhance the security at a particular facility. Cooperation and coordination between the vessel and the terminal should prove beneficial to each. Facility personnel working in conjunction with vessel personnel will frequently know the most appropriate security measures to implement given the differences among facilities and vessels calling at them. Further, the cost of security may be reduced, as duplication of effort will be avoided. This joint effort is highly encouraged.

f. The authority to mandate national, uniform requirements of general applicability for these vessels does not exist until enforceable regulations are promulgated. Until that time, COTPs should seek to gain voluntary compliance with these guidelines as a means of ensuring such uniformity. This can best be accomplished by strongly recommending to vessel owners and operators that they develop security plans incorporating these guidelines.

g. The guidelines are not intended to restrict the lawful exercise of COTP authority to mandate security measures through a COTP order, consistent with paragraph 4.b. below. These guidelines should be considered tools that can be incorporated into a COTP order or security zone, as appropriate.

h. While the guidance contained in this document may assist the industry, public, Coast Guard and other federal and state regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements; nor is it a regulation itself. Thus, it is not intended to nor does it impose legally binding regulatory requirements of general applicability on any party, including the Coast Guard, other Federal agencies, the States or the regulated community.

3. DISCUSSION.

a. Commercial vessels provide a target of opportunity for those desiring to harm the interests of the United States. Owners and operators of vessels have the primary responsibility for ensuring the physical security and safety of their vessels. Therefore, these guidelines are a means of promoting industry practices to advance our vital national security interests. The guidelines do not relieve owners and operators of their legal responsibilities but help them to meet their responsibilities to provide safe and secure transportation for their passengers and cargo.

b. Although the intent is to promote uniform practices and procedures, the guidelines were also drafted with the understanding that threat levels or particular circumstances differ among various geographic areas or ports based upon the risks present. When necessary, COTPs should exercise discretion and flexibility in determining which guidelines are appropriate for a given threat level or the unique circumstances within their zone of responsibility. For example, the COTP may find it necessary to relax a measure prescribed for MARSEC Level 1, as long as adequate security can be assured. On the other hand, a COTP may find it necessary to adopt a MARSEC Level 2 guideline for application in MARSEC Level 1because of heightened concerns that do not necessarily require stepping up to the higher MARSEC Level, but still warrant additional measures.

c. It is anticipated that the International Maritime Organization will finalize maritime security amendments to SOLAS Chapter XI and a new mandatory International Ship and Port Facility Security (ISPS) Code in December 2002. The ISPS Code will also contain a recommendatory part that provides guidance for implementation of the mandatory requirements. Security measures, initiatives and procedures discussed in this circular and addressed in a Vessel Security Plan will also be used to satisfy evolving international vessel security requirements for ships on international voyages. Therefore, specific plan content guidance will be updated after the December IMO meeting for vessel security requirements. The proposed international requirements can be read at http://www.uscg.mil/hq/g-m/imosec.htm.

4. OTHER CONSIDERATIONS.

a. Authority. The primary authority for issuing COTP orders regarding vessel security is the Magnuson Act and its implementing regulations at 33 C.F.R. Part 6. COTP orders related to security may also be issued under the Ports and Waterways Safety Act (PWSA). However, the regulations under the PWSA related to security have not been fully implemented. Although future vessel security regulations will cite the PWSA as additional controlling legal authority, until that time, the Coast Guard retains the longstanding practice of issuing COTP orders based on security concerns under the Magnuson Act.

b. Threshold requirements for exercising COTP authority.

(1) When issuing a COTP order under Magnuson Act regulations, the COTP must find that action "necessary in order to secure such vessel from damage or injury or to

prevent damage or injury to any vessel, or waterfront facility or water of the United States, or to secure the observance of rights and obligations of the United States." With respect to the establishment of a security zone, the authority would additionally extend to actions "necessary . . . to safeguard ports, harbors, or territories . . . of the United States." Simply put, there must be some articulable security threat that encompasses the vessel or facility subject to the order.

(2) The process for assessing the threat and selecting control measures must not be "arbitrary or capricious." Moreover, the requirements imposed by the order or security zone must be reasonable in scope and rationally related to safeguarding the vessel, harbor, port, or waterfront facility from the articulable security threat(s). Normally, COTP orders are specifically tailored for a limited purpose to resolve a specific issue arising under the facts and circumstances involving a particular vessel or facility. For security zones created through temporary final rules, the law requires COTPs to articulate good cause for both the lack of notice and opportunity for public comment and for an effective date less than 30 days after publication.

(3) A finding of necessity under this standard should be based on a careful consideration of the cumulative information available to the COTP. All relevant factors should be considered, including the potential target of the threat, specific geographic or operating conditions that may make a target vulnerable, current intelligence or other threat information, adequacy of voluntary security measures taken by the vessel, and symbolic factors such as periods of national or religious holidays. Each factor may not individually rise to the standard required, but collectively may be sufficient. A generalized threat or warning, reinforced by more specific and credible information related to possible attacks or unlawful acts against a specific type of vessel, could meet the standard enunciated in the Magnuson Act and its implementing regulations.

(4) District legal officers are available to COTPs making decisions to issue COTP orders, or imposing security zones. COTPs should be prepared to pursue sanctions for violations when issuing an order or establishing a security zone. In issuing such orders, COTPs should consider the necessity for the order, the threat that caused it to be issued, and the reasonableness of the required measures as they relate to mitigating that threat (how the required measures will increase security).

c. Application to state vessel operations. Magnuson Act authority can be exercised over vessels owned and operated by a state and political subdivisions of a state. This may include a requirement that persons or vehicles be inspected prior to boarding a vessel. Care should be taken to avoid mandates that would directly compel enactment of state legislation or require the states, in their sovereign capacity, to use law enforcement personnel as a mechanism of enforcing federal law against private individuals. For example, a COTP order that specifically requires local sheriffs or state police to conduct an activity on a vessel, such as vehicle inspections, may violate constitutional principles of federalism. However, issuing a similar order directly to a state owned vessel, without

mandating that state or local law enforcement personnel must conduct vehicle inspections, would pass constitutional scrutiny.

d. Passenger and vehicle inspection. Authority exercised under the Magnuson Act cannot displace the constitutional protections U.S. citizens enjoy, including freedom from unreasonable searches and seizures. However, the guidelines include inspections, which are examinations of passengers, cargo, vehicles, or baggage for the protection of passengers and crew. The purpose of the inspection is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of a similar nature. Such inspections are intended to ensure that incendiary devices, explosives, or other items that pose a real danger of violence or a threat to security are not present. Inspections must be limited and no more intrusive than necessary to protect against the danger of sabotage or similar acts of destruction or violence. The inspection should, however, be reasonably effective to discover incendiary devices, weapons, explosives, and other implements of destruction. Inspection techniques include, but are not limited to, magnetometers, physically examining the person or objects visually or through the use of trained animals, electronic devices, or combination of methods. The inspections must be conducted for a purpose other than the gathering of evidence for criminal prosecutions.

e. Possession of otherwise lawful weapons. There is no federal law *per se* that would prohibit possession of a weapon on board a vessel, provided the weapon is otherwise lawfully carried or permitted under applicable state or local law. There are several options available to the vessel operator to minimize the risk to the vessel by people with weapons. Vessel operators may develop and implement a procedure whereby weapons and ammunition are temporarily relinquished to the vessel operator and placed in a secure location for the duration of the voyage. Of course, the vessel operator may also ban the possession of weapons as a condition of boarding.

f. Public notification. Conspicuous signs should be posted in public places that describe the current security measures being taken to ensure the security of the vessel and persons. For example, when vehicle or personnel inspections are conducted, and when weapons are to be secured during the voyage, the vessel should post visible signs and make appropriate announcements to notify potential passengers and any other personnel of these policies. These signs and announcements should also clearly state that boarding of the vessel is deemed valid consent to the inspection of vehicles, persons, articles and effects. Furthermore, it should be made clear that those failing to give such consent or refusing screening and inspection shall be denied boarding.

PAUL J. PLUTA
Assistant Commandant for Marine Safety,
Security and Environmental Protection

Encl: (1) Security Guidelines for Vessels

Intentionally Left Blank

Intentionally Left Blank

Security Guidelines for Vessels

This Navigation and Vessel Inspection Circular (NVIC) recommends guidelines for performing security assessments, developing security plans, and implementing security measures and procedures.

Commercial vessels provide a target of opportunity for those desiring to harm the interests of the United States. Owners and operators of vessels have the primary responsibility for ensuring the physical security and safety of their vessels. Therefore, these guidelines are a means of promoting industry practices to advance our vital national security interests. The guidelines do not relieve owners and operators of their legal responsibilities but help them to meet their responsibilities to provide safe and secure transportation for their passengers and cargo.

While the guidance contained in this document may assist the industry, public, Coast Guard and other federal and state regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements; nor is it a regulation itself. Thus, it is not intended to nor does it impose legally binding regulatory requirements of general applicability on any party, including the Coast Guard, other Federal agencies, the States or the regulated community.

These guidelines were developed to assist owners and *operators* to establish protective measures that are appropriate to their specific vessel. Understanding that vessels are unique, owners and/or *operators* may seek an alternative to the specific protective measures recommended in Appendix A. A vessel owner and/or *operator* may demonstrate that an alternative to a protective measure provides an acceptable level of protection. Additionally, vessel owner and/or *operator* may seek to demonstrate that specific protective measures recommended in Appendix A are not appropriate for specific vessels (due to vessel design, route, operations, etc.). Appendix B provides a method for owners and/or *operators* to demonstrate that, because of reduced consequence and/or vulnerability, a vessel does not need to mitigate (provide protective measures) a specific activity or objective.

1. Introduction

This Navigation and Vessel Inspection Circular (NVIC) establishes guidelines for vessels for performing security assessments, developing security plans, interfacing with facilities, and implementing security measures and procedures to reduce the risk to passengers, crew and port personnel on board vessels, in port areas, and to the vessels and their cargo. These guidelines address the following elements: awareness, prevention, and response. A vessel's crew should continually be aware of their environment and the domain in which they are operating as the critical first step to prevent acts threatening the security of vessels. Prevention measures are those designed to increase the difficulty of unauthorized boarding, prevent the introduction of *prohibited weapons*, incendiaries, or explosives, and prevent the unauthorized operation of a vessel. A vessel's crew should be prepared to respond within their capabilities to acts that threaten the security of the vessel.

In order to achieve these elements this Circular embodies a number of functional objectives. These include, but are not limited to:

- gathering and assessing information with respect to security threats and exchanging such information with appropriate stakeholders;
- maintaining communication protocols for vessels and facilities;
- preventing or deterring unauthorized access to vessels, facilities, and their *restricted areas*;
- preventing or deterring the introduction of *prohibited weapons*, incendiary devices, or explosives to vessels;
- providing means for raising the alarm in reaction to security threats or security incidents;
- implementing vessel security plans based upon security assessments and the activation of the plans based upon the corresponding threat; and
- training and drills to ensure familiarity with security plans and procedures.

2. Definitions

Note: All words or phrases that have been defined in these guidelines have been italicized throughout the document

For the purpose of this Circular, unless expressly provided otherwise:

Captain of the Port (COTP) means the Coast Guard officer designated by the *Commandant* to command a *Captain of the Port* Zone as described in 33 CFR 1.01-30, or an authorized representative.

Commandant means the *Commandant* of the U.S. Coast Guard as described in 46 CFR 1.01-05.

Company Security Officer (CSO) means a company official from the vessel's owner and/or *operator* who will be responsible for developing, maintaining, and enforcing the company security plans as set out in this document.

Declaration of Security (DOS) is an agreement to be executed between the responsible vessel and waterfront facility and provides a means for ensuring that the critical security concerns are properly addressed and security will remain in place throughout the vessel's activities within the port. Security for the vessel is properly addressed by delineating the responsibilities for security arrangements and procedures between a vessel and waterfront facility.

High Consequence Cargo means any cargo that is a:

- division 1.1 or 1.2 explosive as defined in 49 CFR 173.50 and that is in a quantity in excess of 5,000 kg net explosive weight;
- division 2.3 gas as defined in 49 CFR 172.101 that is a material poisonous by inhalation as defined in 49 CFR 171.8 and that is in a quantity in excess of 10,000 kg;
- division 6.1 liquid as defined in 49 CFR 172.101 that is a material poisonous by inhalation as defined in 49 CFR 171.8 and that is in a quantity in excess of 30,000 kg;
- class 7 radioactive material that is a highway route controlled quantity or fissile material, controlled shipment, as defined in 49 CFR 173.403;
- division 1.5 compatibility group D explosive material for which a permit is required under 49 CFR 176.415, and that is in a quantity in excess of 40,000 kg;
- bulk liquid cargo that is required to be carried in a Type I ship or cargo containment system due to safety hazards under 46 CFR 153; or
- bulk liquefied gas cargo that is flammable and/or toxic and carried under 46 CFR

Inspection means an examination to detect the presence of *prohibited weapons*, dangerous substances and devices that could be used in an *unlawful act* threatening the security of a vessel, port, or waterfront facility.

Maritime Security (MARSEC) Level I means the new maritime security normalcy. This is the level of threat potential for which protective measures may be maintained for an indefinite period of time; in other words, these are the normal, every day security measures.

Maritime Security (MARSEC) Level 2 means there is a heightened threat of a *unlawful act* against a port, waterfront facility, or vessel and intelligence indicates that terrorists are likely to be active within a specific area or against a specific class of target. This risk level indicates that a particular segment of the industry may be in jeopardy, but that no specific target has been identified. Additional protective measures may be expected to be sustained for substantial periods of time.

Maritime Security (MARSEC) Level 3 means the threat of a *unlawful act* against a port, waterfront facility, or vessel is probable or imminent. Intelligence may indicate that terrorists have chosen specific targets, though it may not be possible to identify such targets. Additional protective measures are not intended to be sustained for substantial

periods of time.

Operator means the person, company, or governmental agency, or the representative of a company or governmental agency, which maintains operational control over a vessel covered by this Circular.

Prohibited Weapon means a firearm, knife, or other device or substance that is not permitted on board a vessel or the presence of which is regulated on board a vessel under policy established by the *operator* under their initiative or pursuant to state or local law.

Restricted Area means spaces that are essential to the operation, control, or safety of the vessel.

Suspicious vehicle means a vehicle that by the totality of the circumstances surrounding its appearance or actions, including but not limited to operation contrary to posted guidance and the experience and training of the observing official, presents a particularized and objective basis to suspect that it is engaged unusual or out of the ordinary behavior.

Ship or Vessel Security Officer (hereafter referred to as *Vessel Security Officer*), as appropriate, means the person on board the vessel accountable to the master for the security of the vessel, including implementation and maintenance of the *Vessel Security Plan* and for liaison with the *Company Security Officer* and the waterfront facility.

Unlawful Act means an act that is a felony under U.S. federal law, under the laws of the states where the vessel is located, or under the laws of the country in which the vessel is registered.

Vessel Security Plan means a plan developed to ensure the application of measures on board the vessel designed to protect persons on board, the cargo, or the vessel from the risks of a security incident.

Vessel/waterfront facility interface means the activities that occur when a vessel is directly and immediately affected by an action involving the movement of people, goods or the provisions of port services to or from the vessel.

3. Scope

All vessel operators and owners are encouraged to consider the guidance provided in this Circular. This circular has been developed to assist vessel operators and owners to align with the security requirements being developed at the International Maritime Organization (IMO) and reflect good security practices for all vessels. Therefore, U.S. vessels, including MODUs and public vessels, and foreign vessels calling at U.S. ports would benefit from initiating this guidance which has been specifically developed for all vessels, except:

a. Uninspected vessels other than towing vessels;
b. Passenger vessels required to comply with 33 CFR 120 and 33 CFR 128, which are addressed by NVIC 4-02;
c. Ferries certified to carry more than 500 passengers and addressed by G-M letter 16611 dated 4 Sep 02;
d. Passenger vessels, other than offshore supply vessels as defined in 46 CFR 175.400, inspected under 46 CFR Subchapter T; and
e. Vessels of War.

Fixed and floating platforms are not covered by this guidance. Separate guidance will be published for fixed and floating platforms.

COTPs may encourage vessels, in addition to those vessel specified above, that may pose a risk to the port (due to their type, operations, etc.) to consider this guidance.

4. Alternatives

The Coast Guard recognizes that vessel security plans must be appropriate for a vessel's size, area of operation, and trade. Vessels, other than vessels that engage on international voyages, meeting an industry standard that has been reviewed and accepted by the Commandant (G-MPS) as providing an appropriate standard of security for that vessel type will be considered to meet the guidance in this NVIC.

Vessel owners and/or operators that participate in the U.S. Customs Service program titled "Customs Trade Partnership Against Terrorism" (C-TPAT) may be considered to address cargo security concerns discussed in this guidance.

5. Maritime Security (MARSEC) Levels

Maritime Security (MARSEC) Levels were established to allow the Coast Guard to easily and clearly communicate the extent of threat present in a port. *MARSEC levels* also permit the *Captain of the Port* (COTP) and the port community to plan and pre-designate appropriate postures for each level of threat.

These levels are similar to the security levels used in 33 CFR 120, Security of Passenger Vessels. They have also been proposed to International Maritime Organization (IMO) as the international maritime standard. Currently, the Coast Guard is using a three-tiered system.

In March 2002, the President announced a national system for communicating threat levels, the Homeland Security Advisory System (HSAS). Homeland Security Presidential Directive (HSPD) – 3 defines a five-tiered system for setting threat levels. Presently, *MARSEC* is linked to HSAS and serves as the maritime sector's tool for communicating risk. MARSEC Level 1 corresponds to the HSAS Low: Green,

Guarded: Blue, and Elevated: Yellow. MARSEC Level 2 corresponds to HSAS High: Orange and MARSEC Level 3 corresponds to HSAS Severe: Red.

6. USCG and COTP Responsibilities

While the intent of this guideline is to present a broad-based approach to security, invariably there will be threats to the vessel necessitating deviation from this guideline. Accordingly, flexibility in the protective measures may be required to counter specific threats. Where practicable, *operators* may make necessary preparatory steps to develop security measures for emerging threats. At heightened MARSEC levels additional protective measures may be called for as determined locally in cooperation with Federal, state, and local authorities and the industry. This may include changing port calls, not embarking passengers, curtailing cargo operations, or other appropriate measures.

Through existing regulations in 33 CFR Part 6, the COTP retains the authority to issue written requirements for increased security measures to counter a specific threat. This authority may be used to implement measures such as controlling vessel movement in the port, establishing security zones, requiring vessel escorts or hiring additional private security guards.

7. Company Security Officer

The Company may designate a *Company Security Officer*. The *Company Security Officer* may be a collateral duty of a person within a Company, provided they are able to perform the duties and responsibilities required of the *Company Security Officer*.

The duties and responsibilities of the *Company Security Officer* may include, but are not limited to:

- advising what threats may be encountered by the vessel, using appropriate security assessments and other relevant information;
- ensuring that vessel security assessments and annual reassessments are carried out;
- ensuring the development and maintenance of the V*essel Security Plan*;
- modifying the *Vessel Security Plan* to correct deficiencies and satisfy the security requirements of the individual vessel;
- enhancing security awareness and vigilance;
- ensuring adequate training for personnel responsible for the security of the vessel;
- coordinating implementation of the *Vessel Security Plan* with the *Vessel Security Officer* and the relevant designated representative on behalf of the waterfront facility;
- coordinating and ensuring consistency between security requirements and safety requirements;
- ensuring that, if sister-vessel or fleet security plans are used, the plan for each vessel reflects the vessel-specific information accurately; and

- ensuring that any alternative or equivalent arrangements approved for a particular vessel or group of vessels are implemented and maintained.

8. Vessel Security Officer

A *Vessel Security Officer* may be designated, such as by name or position, on each vessel. The *Vessel Security Officer* may be a collateral duty of a crewmember on the vessel and may also be the *Company Security Officer*, provided they are able to perform the duties and responsibilities required of the *Vessel Security Officer*.

Unmanned barges do not need to have a *Vessel Security Officer*. For unmanned barges, the duties and responsibilities below may be performed by the *Company Security Officer*, another designated individual, or the towing vessel's *Vessel Security Officer*, as appropriate, and may be addressed in the *Vessel Security Plan*.

The duties and responsibilities of the *Vessel Security Officer* may include, but are not limited to:

- regular security inspections of the vessel;
- implementing, maintaining, and supervising the *Vessel Security Plan*;
- proposing modifications to the vessel security plan;
- enhancing security awareness and vigilance on board;
- ensuring that adequate training has been provided to vessel personnel;
- coordinating implementation of the *Vessel Security Plan* with the *Company Security Officer* and the relevant designated representative on behalf of the waterfront facility;
- ensuring that security equipment onboard the vessel or associated with vessel security is properly operated, tested, calibrated and maintained; and
- reviewing and completing a *Declaration of Security* agreement.

9. Vessel Security Assessment

The Vessel Security Assessment is an essential and integral part of the process of developing and updating the V*essel Security Plan.* (B8.1)The *Company Security Officer* should ensure that a Vessel Security Assessment is carried out for each vessel in the companies fleet. The *Company Security Officer* need not necessarily personally undertake all the duties associated with performing an assessment. The Vessel Security Assessment includes an on-scene security survey and at least the following elements:

- identification of existing security and response measures, procedures, and operations;
- identification and evaluation of key vessel operations, including sensitive areas that should be designated as *restricted areas*;
- identification of possible threats to the vessel and the likelihood of their occurrence, in order to establish and priortize security measures; and

- identification of weaknesses or vulnerabilities on the vessel, including human factors in the infrastructure, policies and procedures.

The Security Assessment and on-scene security survey may be documented and retained by the *Company Security Officer.*

Prior to commencing the Security Assessment, the *Company Security Officer* may take advantage of information available on the assessment of threat for the ports at which the vessel will call and about the facilities and their protective measures. The *Company Security Officer* may study previous reports on similar security needs. Where feasible, the *Company Security Officer* may meet with appropriate persons on the vessel and in the facilities to discuss the purpose and methodology of the assessment.

Appendix B may be used to aid vessel owner and/or *operator* in performing a security assessment.

The *Company Security Officer* may obtain and record the information required to conduct an assessment, including:

- the general layout of the vessel;
- the location of areas which should have restricted access, such as bridge, engine-room, radio room, steering gear spaces, etc.;
- the location and function of each actual or potential access point to the vessel;
- the location of areas potentially suitable for harboring stowaways or other personnel unlawfully aboard the vessel;
- the open deck arrangement including the height of the deck above the water and, when alongside at any waterfront facility regularly served, the height to the quay at various levels of the tide and at various stages of cargo working;
- the cargo spaces and stowage arrangements;
- the location where the vessels supplies and essential maintenance equipment is stored;
- the locations where unaccompanied baggage is stored;
- the emergency and stand-by equipment available to maintain essential services;
- numerical strength, reliability, and security duties of the vessel's crew;
- existing security and safety equipment for protection of passengers and crew;
- evacuation routes and passenger assembly points which have to be maintained to ensure the orderly and safe emergency evacuation of the vessel;
- existing agreements with private security companies providing vessel/waterside security services at all *MARSEC levels*; and
- existing protective measures and procedures in effect, including inspection, control and monitoring equipment, personnel identification

documents, communication, alarm, lighting, access control, and other appropriate systems.

On-scene security survey

The *Company Security Officer* may ensure that each vessel's protective measures, procedures, and operations are examined and evaluated for:

- ensuring the performance of all vessel security duties;
- monitoring *restricted areas* to ensure that only authorized persons have access;
- controlling access to the vessel;
- monitoring of deck areas and areas surrounding the vessel;
- controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and crew's personal effects);
- supervising the handling of cargo and vessel's stores and bunkers; and
- ensuring that port-specific security communication, information, and equipment are readily available.

The *Company Security Officer* may ensure that each vessel is examined and evaluated to identify each point of access, including open weather decks, and its potential for use by individuals who might be engaged in *unlawful act*. This includes individuals having legitimate access as well as those who seek to obtain unauthorized entry.

The *Company Security Officer* may ensure that existing protective measures, procedures, and operations, are examined and evaluated under both emergency and routine conditions, including:

- established security guidance;
- response procedures to security, fire, or other emergency conditions;
- the level of supervision of the vessel's crew, vendors, repair technicians, dock workers, etc.;
- the frequency and effectiveness of security patrols;
- the security key-control and other access control systems;
- security communications systems and procedures;
- security doors, barriers, and lighting; and
- Surveillance equipment, if installed.

Key vessel operations that are important to protect may include:

- cargo and vessel stores operations;
- navigation, machinery spaces, and steering control stations ; and
- crew and passenger safety.

Possible threats to key vessel operations may include:

- bombing;
- sabotage;

- hijacking;
- unauthorized use;
- smuggling;
- cargo tampering;
- stowaways;
- piracy;
- hostage taking;
- vandalism;
- transporting weapons of mass destruction;
- use of the vessel to carry perpetrators and their equipment; and
- use of the vessel as a weapon.

Identification of vulnerabilities which may include:

- conflicting policies between safety and security measures;
- conflicting vessel and security duty assignments;
- watchkeeping and manning constraints with implications on crew fatigue and alertness;
- training deficiencies; and
- insufficient, poorly maintained or poor quality security equipment.

10. Vessel Security Plan

Each vessel owner and/or operator should develop an effective security program that relies on detailed procedures clearly delineating the preparation, prevention, and response activities that will occur at each threat level along with the organizations, or personnel, who are responsible for carrying out those activities. The vessel owner and/or operator should document the security program in the form of a vessel security plan. While the security plan need not include all of the detailed procedures for the various activities, these procedures may be clearly referenced within the plan framework. This latter step is necessary to establish common links among the overall awareness, training, and execution of the security program.

A *Vessel Security Plan* should contain a clear statement emphasizing the master's authority. The Company may establish in the *Vessel Security Plan* that the master has the overriding authority and responsibility to make decisions with respect to the security of the vessel and to request the assistance of the Company.

The *Company Security Officer* should develop a security plan for each vessel. In formulating a vessel's security plan, the *Company Security Officer* should: (1) perform a comprehensive security assessment and (2) based on this assessment, develop a *Vessel Security Plan* that implements appropriate security measures and procedures for the three *MARSEC levels* that with reasonable confidence will achieve the goals and objectives set out in this Circular. Appendix C provides a generic *Vessel Security Plan* outline that may aid a vessel or company in developing a Vessel Security Plan.

The Company should ensure that the *Company Security Officer*, the master, and the *Vessel Security Officer* are given the necessary support to fulfill their duties and responsibilities in accordance with this Circular. Maintaining ship security is an ongoing task. Additional security measures may be implemented to counter increased risks when warranted.

These guidelines were developed to assist owners and/or *operators* to establish protective measures that address the below activities and objectives appropriate to their specific vessel. Understanding that vessels are unique, owners and/or *operators* may seek an alternative to the specific protective measures recommended in Appendix A. A vessel owner and/or *operator* may demonstrate that an alternative to a protective measure provides an acceptable level of protection. Additionally, vessel owner and/or *operator* may seek to demonstrate that specific protective measures recommended in Appendix A are not appropriate for specific vessels (due to vessel design, route, operations, etc.). Appendix B provides a method for owners and/or *operators* to demonstrate that, because of reduced consequence and vulnerability, a vessel does not need to mitigate (provide protective measures) a specific activity or objective.

At *MARSEC Level 1*, the owner and/or *operator* may consider the following activities, through appropriate broad protective measures, as provided in Appendix A, to identify and take preventive measures against security incidents and increase awareness of general threats:

- ensuring the performance of all vessel security duties;
- monitoring *restricted areas* to ensure that only authorized persons have access;
- controlling access to the vessel;
- monitoring of deck areas and areas surrounding the vessel;
- controlling the embarkation of persons and their effects;
- supervising the handling of cargo and vessel's stores and bunkers; and
- ensuring that port-specific security communication is readily available.

At *MARSEC Level 2*, in addition to *MARSEC Level 1* protective measures, the owners and/or *operators* may consider the protective measures provided in Appendix A to extend the area of awareness and increase surveillance measures for each activity, to rapidly and effectively identify and take preventive measures against security incidents.

At *MARSEC Level 3*, in addition to *MARSEC Level 1* and 2 protective measures, the owner and/or *operator* may consider the protective measures provided in Appendix A to increase surveillance while significantly restricting access to immediately identify and respond to security incidents.

The *Vessel Security Plan* may address procedures for response to mitigate threats identified in the Vessel Security Assessment. The owner and/or *operator* may consider developing scenario-based response measures for acts threatening the security of the vessel. These measures are not limited to but may address the following:

- securing all access to the vessel to prevent intrusion;

- performing emergency shutdown of main engine(s) to prevent unauthorized operation;
- securing non-critical operations to focus attention on response;
- alerting vessel and shore-side authorities of an incident;
- rendering assistance to a nearby vessel undergoing an *unlawful act* that threatens its security;
- responding to the detection of stowaways or intruders;
- repelling boarders;
- addressing a malfunction of on board security equipment;
- screening the underwater hull or search the vessel in response to bomb threats;
- specifying the kind of communications to use in the event of a breach of security, an *unlawful act*, or other emergency; and
- coordinating with waterfront facility response procedures.

When a vessel is in a period of extended maintenance (e.g., dry-docking) and/or is out of service, the owner and/or *operator* may consider to reduce the security measures recommended by this circular on the basis that there is reduced risk to passengers, crew, cargo, port personnel, infrastructure in port areas, or the environment. The *Vessel Security Plan* may address the measures and processes for both placing a vessel in a period of extended maintenance and placing a vessel back in service.

The *Vessel Security Plan* may be developed taking into account the guidance given in this Circular. The plan may consist at least of, but is not limited to:

- measures and/or equipment designed to prevent or deter *prohibited weapons*, dangerous substances and devices intended for use against people, vessels or ports and the carriage of which is not authorized from being introduced by any means on board the vessel;
- identification of the *restricted areas* and measures and/or equipment for the prevention of unauthorized access to the vessel and to *restricted areas* on board;
- procedures for responding to security threats or breaches of security, including those scenario-based responses provided above, provisions for maintaining critical operations of the vessel, or *vessel/waterfront facility interface*;
- procedures in case of security threats or breaches of security that might require evacuation of a vessel;
- duties of vessel personnel assigned security responsibilities and duties;
- procedures for auditing the security activities, procedures for training, and exercises and drills associated with the plan;
- procedures for interfacing with other vessels or waterfront facility security activities;
- procedures for the periodic review of the plan and for updating;
- procedures for reporting security incidents;
- identification of the *Vessel Security Officer* and Company Security

Officer;
- procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board; and
- procedures for reporting, responding, and addressing stowaways and detained crew members.

The *Vessel Security Plan* may be combined with other safety management systems such as those required by SOLAS in chapter IX. The plan may be kept in an electronic format. In such a case, it should be protected by means to prevent it from being deleted, destroyed or overwritten.

The Company should establish procedures to restrict the distribution, disclosure, and availability of information contained in the plan. Access to the plans should be restricted to those persons with an operational need to know. A copy of the *Vessel Security Plan* may normally be kept aboard each vessel in a secure location and may be made available to the COTP.

11. Non Self-propelled Vessels

The responsibility for barge security starts with the barge owner and/or operator, but in reality, the towing vessel, fleeting area, and waterfront facility where the barge is moored all share this responsibility. Barge owners may consider as a factor in the selection of a towing company the towing company's procedures to ensure the security of barges in its care.

Similarly, barge and towing vessel owners may consider the security procedures of fleeting areas and facilities and work with fleet and waterfront facility operators to ensure the security of barges in their care. Barge owners and/ or operators that transport *High Consequence Cargos* should consider ensuring that barges are provided continuous surveillance while in transit, moored at fleeting areas, or moored at waterfront facilities.

Barge and towing vessel companies may have *Vessel Security Plans*, as discussed in section 10, which apply to their entire fleet, where vessel type and operations are similar.

12. Records

Records of the following activities addressed in the *Vessel Security Plan* may be maintained and made available to the COTP upon request:
- details of training, drills, and exercises;
- reports of security incidents;
- report of breaches of security or suspicious activities;
- changes in *MARSEC levels* including the date and port;
- maintenance, calibration, and testing of security equipment; and
- periodic review of the security survey.

13. Training and Drills

The *Company Security Officer*, *Vessel Security Officer*, and appropriate shore-based personnel generally should have knowledge and receive training taking into account the guidance given in this Circular. Vessel personnel having specific security duties and responsibilities should understand their responsibilities for vessel security as described in the *Vessel Security Plan* and generally have sufficient knowledge and ability to perform their assigned duties. Training may include, but is not limited to, the following, as appropriate:

- security administration;
- relevant international conventions, codes, and recommendations;
- responsibilities and functions of other involved organizations;
- relevant government legislation and regulations;
- risk, threat, and vulnerability assessments;
- security surveys and inspections;
- vessel and waterfront facility security measures;
- recognition of characteristics and behavioral patterns of persons who are likely to commit *unlawful act*;
- inspection, control and monitoring techniques;
- techniques used to circumvent security measures;
- recognition and detection of *prohibited weapons*, dangerous substances and devices;
- vessel and local port operations and conditions;
- security devices and systems; and
- methods, policy, and procedures of physical searches.

Drills and exercises may be conducted monthly to ensure the adequacy of the Vessel Security Plan.

14. Declaration of Security

The *Declaration of Security* provides a means for ensuring that critical security concerns are properly addressed and security will remain in place throughout the vessel's activities within the port. Security is properly addressed by delineating responsibilities for security arrangements and procedures between a vessel and waterfront facility. This obligation is similar to the existing U.S. practice for vessel/waterfront facility oil transfer proceedings.

Vessels carrying *High Consequence Cargoes* should complete a DOS for every interface, regardless of the MARSEC Level. At MARSEC Level 2 and 3, guidance for which *vessel/waterfront facility interfaces* are encouraged to complete a *Declaration of Security* will be published in a NVIC on Recommended Security Guidelines for Waterfront Facilities. The COTP, may adjust this submission recommendation, after assessing the

risk a *vessel/waterfront facility interface* poses to people, property, or the environment.

The *Declaration of Security* may be completed by:

- the master, *Vessel Security Officer,* or designated person on behalf of the vessel; and
- the designated representative on behalf of the waterfront facility.

The *Declaration of Security* generally addresses the protective measures for the waterfront facility and vessel and the responsibility for each. Both the vessel and the waterfront facility generally keep a copy of the Declaration of Security. The *Declaration of Security* may be made available to the COTP or their representative upon request. An example of a *Declaration of Security* is provided in Appendix D.

For vessels that frequently call upon the same waterfront facility, a *Declaration of Security* for each interface is not required if the vessel and waterfront facility enter into a written agreement stating the responsibility for each during the *vessel/waterfront facility interface*. These agreements may be included in the *Vessel Security Plan* and the waterfront facility security plan.

Appendix A

Guidance on Establishing Protective Measures

This appendix provides guidance on establishing protective measures that may be implemented by a vessel to achieve those goals and objectives set out in Enclosure (1). This guidance is based on existing guidance provided in Navigation and Vessel Inspection Circulars, best practices from industry standards, and the United States position as proposed to the International Maritime Organization (IMO), and is presently being discussed for implementation into an International Code for the Security of Ships and Port Facilities.

As discussed in Enclosure (1), owners and/or *operators* may provide an alternative to or demonstrate that a specific protective measure recommended in this appendix is either unnecessary or not appropriate for this vessel's design and/or service.

Where protective measures are provided in a table, a vessel owner and/or *operator* may select the appropriate protective measure or combination of protective measures allowing the vessel to achieve an acceptable level of protection for each activity or objective. However, a vessel may consider implementing those protective measures that are indicated with a "YES" in a table. For example, a vessel may monitor their *restricted areas*. This may be accomplished through the use of, or a combination of, protective measures in table 2. While locking or securing access to a *restricted area* may be a more passive protective measure and possibly the most reliable solution, using a combination of security personnel and an intrusion alarm may provide an acceptable level of protection for a specific vessel type at *MARSEC Level 1*.

Security measures and initiatives may be incorporated into existing crewmembers duties and responsibilities. For example, fire patrols or roving engineering and deck watch standers that make rounds may perform security patrol duties and responsibilities during the normal and every day performance of their existing duties.

Ensuring the performance of all vessel security duties

1.1 Vessels may incorporate relevant security elements into the duties and responsibilities of all watchstanders. Such elements may include, but not be restricted to:

.1 heighten awareness that includes observing and reporting malfunctioning security equipment, suspicious persons, objects, and activities during rounds; and

.2 additional duties as required by the vessel security plan.

1.2 The following table provides additional guidance on protective measures and procedures for ensuring the performance of all vessel security duties.

Table 1

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
All vessel crewmembers normally review and exercise their security duties and responsibilities through drill and training	**YES***	**YES***	**YES***
Provide security information to all crewmembers and any security personnel that includes the security level and any specific threat information	**Optional**	**YES**	**YES**
Vessel Security Officer should normally communicate with the waterfront facility to coordinate protective measures	**YES**	**YES#**	**YES#**
*Drills and exercises may be conducted monthly. #Coordinate additional protective measures.			

Monitoring restricted areas to ensure that only authorized persons have access

1.3 Vessels may establish *restricted areas* to control access to key areas. The following areas may be designated *restricted areas* and may be listed in the *Vessel Security Plan*:

.1 navigational bridge;
.2 control stations and central control station;
.3 machinery spaces containing propulsion machinery, generators and major electrical machinery, main and auxiliary steering gear, ventilation and air-conditioning machinery and similar spaces;
.4 spaces with access to potable water tanks, pumps, or manifolds;
.5 cargo pump-room; and
.6 any other areas as determined by the *Company Security Officer* to which access may be restricted to maintain the security of the vessel.

1.4 All *restricted areas* may be marked indicating that the area has restricted access. Markings do not need to be conspicuous to persons other than the crew.

1.5 Monitoring of *restricted areas* may be accomplished by protective measures in table 2.

Table 2

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Locking or securing access to *restricted areas*@	**Optional**	**YES**	**YES**
Using personnel as security guards or patrols	**Optional**	**YES***	**YES#**
Increasing the frequency and detail of monitoring of *restricted areas* may include: *Dedicating personnel to guarding or patrolling *restricted areas*; and #Posting personnel to continuously guard *restricted areas* and/or assigning personnel to continuously patrol *restricted areas* and areas adjacent to restricted areas. @ Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.			

Additional protective measures to monitor *restricted areas* may include:

.1 using surveillance equipment, such as closed circuit television (CCTV); or

.2 using automatic intrusion detection devices to alert the crew of unauthorized access to *restricted areas*.

1.6 When automatic intrusion detection devices are used to monitor unauthorized access to *restricted areas*, automatic intrusion detection devices may:

.1 activate an audible and/or visual alarm;

.2 indicate in a location that is continuously staffed or monitored; and

.3 be regularly tested.

Controlling access to the vessel

1.7 When implementing protective measures the following access points may be considered:

.1 ladders;

.2 gangways;

.3 side ports;

.4 adjacent piers and aprons; and

.5 other access points identified in the vessel security assessment.

1.8 Vessels may implement the protective measures or combination of protective measures provided in the table below to control access to the vessel.

Table 3

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Access points are normally secured[@] or continuously attended to prevent unauthorized access	**YES**	**YES[#]**	**YES[#]**
Weather-deck access vents, storage lockers, and doors to normally unmanned spaces (such as storerooms, auxiliary machinery rooms, etc.) may be locked[@] or precautions taken to prevent unauthorized access	**YES**	**YES**	**YES**
Limit entry to the vessel to a minimum number of access points[+]	**Optional**	**YES**	**YES***
Coordinate with the waterfront facility to extend access control beyond the immediate area of the vessel	**Optional**	**YES**	**YES**

*Limit entry to a single access point.
[@] Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.
[+] While not restricting egress from the vessel in the event of an emergency.
[#] Assign additional personnel at appropriate access points as designated in the security plan.

1.9 Access may be denied to any person refusing to submit to security verification or inspection at a point of access. Each person denied entry for refusing may be identified and reported to appropriate authorities.

Monitoring of deck areas and areas surrounding the vessel

1.10 Vessel capabilities normally include the ability to perform monitoring at all times and in all conditions.

1.11 Monitoring of deck areas and areas surrounding the vessel to identify and take preventive measures against security incidents vessels may be accomplished by using:

.1 equipment, such as alarms and CCTV; or

.2 personnel, such as security patrols.

Table 4

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Use security lookouts and/or security patrols	**Optional**	**YES**	**YES***
Perform waterside boat patrols	**Optional**	**Optional**	**YES***
Use divers to inspect the underwater pier structures prior to the vessel's arrival, upon the vessel's arrival, and in other cases deemed necessary	**Optional**	**Optional**	**YES**
* Increase the number and frequency of: .1 security patrols to ensure continuous monitoring; and .2 waterside boat patrols to ensure continuous monitoring.			

1.12 Vessels may consider illuminating their deck and access points to the vessel while conducting vessel/waterfront facility interface activities. Vessels may coordinate lighting with other entities involved in the vessel/waterfront facility interface. While underway, vessels may consider using the maximum lighting available consistent with safe navigation. A vessel may consider the following in establishing the appropriate level and location of lighting:

.1 crewmembers are generally able to see beyond the vessel, both pier side and waterside; and

.2 coverage normally includes the area on and around the vessel.

1.13 At heightened *MARSEC levels*, additional lighting may be coordinated with the waterfront facility to provide additional shore side lighting. Additional lighting may include:

.1 using spotlights and floodlights to enhance visibility of the deck and areas surrounding the vessel; and

.2 using lighting to enhance visibility of the surrounding water and waterline.

Controlling the embarkation of persons and their effects

1.14 Controlling the embarkation of persons and their effects to adequately identify and take preventive measures against security incidents may include the protective measures provided in the following table.

Table 5

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Verify reason personnel are embarking the vessel by using tickets, boarding passes, work orders, or other means	**YES**	**YES**	**YES**
Positively identify crewmembers, passengers, vendors, visitors, and other personnel prior to each embarkation	**YES**	**YES**	**YES**
Arriving crew verified as authorized to serve aboard the vessel	**YES**	**YES**	**YES**
Inspect persons, baggage, carry-on items, and personal gear for *prohibited weapons*, incendiaries, and explosives	**YES#**	**YES@**	**ALL**
Security briefings provided to all passengers, prior to departing, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities	**Optional**	**YES**	**YES***
Assign personnel to guard designated *inspection* areas	**Optional**	**YES**	**YES**
Limit entry to only passengers and crewmembers	**Optional**	**Optional**	**YES**
Escort all service providers or other personnel needed aboard to provide essential services to the vessel	**Optional**	**Optional**	**YES**
*Security briefings are generally provided to all passengers, prior to each embarkation and disembarking. #This may be accomplished by random *inspections*, such as 5-20% or some other method addressed in the vessel security plan. @Increase the frequency, such as 25-50%, and detail of *inspections*.			

1.15 Areas should be designated to inspect baggage, carry-on items, and personal gear. Access to and from these areas should be controlled to segregate inspected persons and articles from un-inspected persons and articles.

1.16 The purpose of the inspection is for private entities to secure their personal safety and safety of their property. Such inspections are intended to ensure that incendiary devices, explosives, or other items that pose a real danger of violence or a threat to security are not present. Inspections may be limited and no more intrusive than necessary to protect against the danger of sabotage or similar acts of destruction or violence. The inspection may, however, be reasonably effective to discover incendiary devices, weapons, explosives, and other implements of destruction. Inspection techniques may include, but are not limited to, magnetometers, physically examining the person or objects visually or through the use of trained animals, electronic devices, or combination of methods.

Supervising the handling of cargo and vessel's stores

1.17 Vessels may use the following table as guidance on supervising the handling of cargo and vessel's stores and bunkers to adequately identify and take preventive measures against security incidents.

Table 6

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Verify non-containerized cargo against the manifest°	**YES#**	**ALL**	**ALL**
Verify the container identification numbers of loaded containers against the manifest°	**ALL**	**ALL**	**ALL**
Verify the container identification numbers of empty containers against the manifest°	**YES#**	**ALL**	**ALL**
Inspect vessel's stores and provisions	**YES#**	**YES+**	**ALL**
#This may be accomplished by random verification, such as 25-50% of cargo. +Increase the frequency and detail of *inspection*, such as 25-50%. °Companies are encouraged to participate in the U.S. Customs Service program titled "Customs Trade Partnership Against Terrorism" (C-TPAT).			

1.18 Verification and *inspection* of cargo and vessel's stores may be accomplished by:

.1 visual and physical examination;

.2 using scanning/detection equipment, mechanical devices, or canines; or

.3 coordinating with the shipper or other responsible party through an established agreement and procedures.

At heightened *MARSEC levels*, the detail of the above methods may be increased commensurate to the threat.

Ensuring that port-specific security communication is readily available

1.19 Vessels normally ensure that means of communication to report acts threatening the security of the vessel are:

.1 maintained and operable;

.2 readily available;

.3 able to communicate within the vessel, to the waterfront facility, and with appropriate law enforcement personnel; and

.4 able to relay essential information related to the nature and extent of the threat.

1.20 At heightened *MARSEC levels*, vessels may enhance their means of communication to report acts threatening the security of the vessel as provided in the following table.

Table 7

	MARSEC Level		
Protective Measure	**1**	**2**	**3**
Perform regular communications checks	**Optional**	**YES**	**YES**
Provide a backup means of communication	**Optional**	**YES**	**YES#**
# Provide a redundant and multiple means of communication			

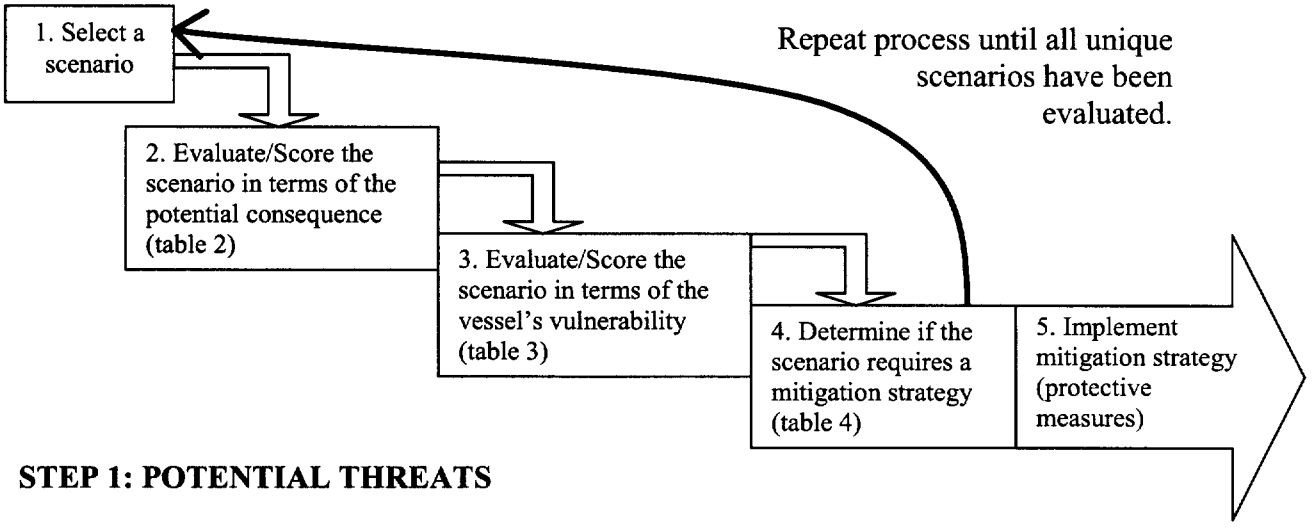
Appendix B

Guidance on Performing Security Assessments

It is generally agreed that risk-based decision-making is one of the best tools to complete a security assessment and to determine appropriate security measures for a vessel. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions to reduce the vulnerability and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a security assessment might reveal weaknesses in an organization's security systems or unprotected access points such as the pilot boarding ladder not being raised or side ports not being secured or monitored after loading stores. To mitigate this threat, a vessel would implement procedures to ensure that such access points are secured and verified by some means. Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to *restricted areas* to prevent unauthorized personnel from entering such spaces. Such assessments can identify vulnerabilities in vessel operations, personnel security, and physical and technical security.

The following is a simplified risk-based security assessment that can be further refined and tailored to specific vessels. The process and results may be documented when performing the assessment. An example is provided in Table 5 on how to document the process and results.



STEP 1: POTENTIAL THREATS

To begin an assessment, a vessel or company needs to consider attack scenario(s) consisting of a potential threat to the vessel under specific circumstances. It is important

that the scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as given by a threat assessment. For example, a boat containing explosives (a specific attack scenario) ramming a tanker (target) that is outbound through a choke point (specific circumstance) is one credible scenario. It may be less credible that a hand held missile launched from a distance at a large tanker could intentionally sink the vessel that is outbound through a choke point.

The number of scenarios is left to the judgment of the vessel owner and/or *operator*. An initial evaluation should at least consider those scenarios provided in Table 1 with emphasis being placed on the worst-case scenario, and the most probable scenarios. Care should be taken to avoid unnecessarily evaluating excessive scenarios that result in low consequences. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences.

Table 1: Notional List of Scenarios

Typical Types of Scenarios		Application Example
1. Intrude and/or take control of the target and ...	a. Damage/destroy the vessel with explosives	Intruder plants explosives.
	b. Damage/destroy the vessel through malicious operations/acts	• Intruder takes control of a vessel and runs it aground or collides with something intentionally. • Intruder intentionally opens valves to release Hazmat, etc.
	c. Create a hazardous or pollution incident without destroying the vessel	• Intruder opens valves/vents to release toxic materials or releases toxic material brought along. • Intruder overrides interlocks leading to damage/destruction.
	d. Take hostages/kill people	Goal of the intruder is to kill people.
2. Externally attack the vessel by ...	a. Moving explosives adjacent to vessel • From the waterside • On the shore side • Subsurface	• USS Cole style attack. • Car/truck bomb.
	b. Ramming a stationary target: • With a vessel • With a land-based vehicle	Intentional allision meant to damage/destroy the target (i.e. waterway choke point). NOTE: Evaluate overall consequences from the allision, but only evaluate the vulnerabilities of the vessel and not the vulnerabilities of the target being rammed.
	c. Launching or shooting weapons from a distance	Shooting at a vessel using a rifle, missile, etc.
3. Use the vessel as a means of transferring ...	a. Materials to be used as a weapon into/out of the country	
	b. People into/out of the country	

STEP 2: CONSEQUENCE ASSESSMENT

Each scenario should be evaluated in terms of the potential consequences of the attack. Three elements are included in the consequence assessment: death and injury, economic impact, and environmental impact. A descriptor of the consequence components follows:

DEATH AND INJURY	The potential number of lives that could be lost and injuries occurring as a result of an attack scenario.
ECONOMIC IMPACT	The potential economic impact of an attack scenario.
ENVIRONMENTAL IMPACT	The potential environmental impact of an attack scenario.

The appropriate consequence score or "rating", should be evaluated for each scenario. Consequence ratings and criteria with benchmarks are provided in the following table. These ratings are intended to be broad relative estimates. The appropriate rating is determined by using the consequence component that results in the highest rating. For example, if the death and injury and economic impact result in a Moderate or "1" rating but the environmental impact result is a Significant or "2" rating, then the over all consequence score would be assigned a rating of "2." A precise calculation of these elements is not necessary.

Table 2: Consequence Score

Assign a rating of:	If the impact could be
3	CATASTROPHIC = numerous loss of life or injuries, major national or long term economic impact, complete destruction of multiple aspects of the eco-system over a large area
2	SIGNIFICANT = multiple loss of life or injuries, major regional economic impact, long-term damage to a portion of the eco-system
1	MODERATE = little or no loss of life or injuries, minimal economic impact, or some environmental damage

STEP 3: VULNERABILITY ASSESSMENT

Each scenario should be evaluated in terms of the vessel's vulnerability to an attack. Four elements of the vulnerability score are: availability, accessibility, organic security, and vessel hardness. With the understanding that the vessel owner and/or *operator* has the greatest control over the accessibility and organic security elements, these elements may be addressed for each scenario. Descriptors of these two vulnerability elements follow:

ACCESSIBILITY	Accessibility of the vessel to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
ORGANIC SECURITY	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.

The vessel owner and/or *operator* should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability is normally viewed with only existing strategies and protective measures, meant to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures considered. Assessing the vulnerability with only the existing strategies and protective measures provides a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate risk.

The vulnerability score and criteria with benchmark examples are provided in the following table. Each scenario should be evaluated to get the individual score for each element and then sum these elements to get the total vulnerability score (step 3 in Table 5). This score should be used as the vulnerability score when evaluating each scenario in the next step.

Table 3: Vulnerability Score

Category	Accessibility	Organic Security
3	No deterrence (e.g. unrestricted access to vessel and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
2	Good deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of vessel)	Good deterrence capability (e.g. minimal security plan, some communications, armed guard force of limited size relative to the vessel; outside law enforcement not available for timely prevention, limited detection systems)
1	Excellent deterrence (expected to deter attack; access restricted to within 500 yards of vessel; multiple physical/geographical barriers)	Excellent deterrence capability expected to deter attack; covert security elements that represent additional elements not visible or apparent)

STEP 4: MITIGATION

The vessel owner and/or *operator* should next determine which scenarios may have mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequence and vulnerability assessment scores. Following are terms used in Table 4 as mitigation categories:

"Mitigate" means that mitigation strategies, such as security protective measures and/or procedures, may be developed to reduce risk for that scenario. An appendix to the *Vessel Security Plan* may contain the scenario(s) evaluated, the results of the evaluation, a

description of the mitigation measure evaluated, and the reason mitigation measures were or were not chosen.

"Consider" means that the scenario should be considered and mitigation strategies should be developed on a case-by-case basis. The *Vessel Security Plan* may contain the scenario(s) evaluated, the results of the evaluation, and the reason mitigation measures were or were not chosen.

"Document" means that the scenario may not need a mitigation measure at this time and therefore needs only to be documented. However, mitigation measures having little cost may still merit consideration. The security plan may contain the scenario evaluated and the results. This will be beneficial in further revisions of the security plan, to know if the underlying assumptions have changed since the last edition of the security assessment.

Table 4 is intended as broad, relative tool to assist in the development of the vessel security plan. "Results" are not intended to be the sole basis to trigger or waive the need for specific measures, but are one tool in identifying potential vulnerabilities and evaluating prospective methods to address them.

Table 4: Vulnerability & Consequence Matrix

		Total Vulnerability Score		
		2	3-4	5-6
	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

To assist the vessel owner and/or *operator* in determining which scenarios may require mitigation methods, the vessel owner and/or *operator* may find it beneficial to use Table 5 provided below. The vessels owner and/or *operator* can record the scenarios considered, the consequence score (Table 2), outcome of the each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category Table 4).

Table 5

MITIGATION DETERMINATION WORKSHEET					
Step 1	Step 2	Step 3			Step 4
Scenario/Description	Consequence Score (Table 2)	Vulnerability Score (Table 3)			Mitigation Results (Table 4)
		Accessibility	+ Organic Security	= Total Score	

STEP 5: IMPLEMENTATION METHODS

The true value of these assessments is realized, once the vessel owner and/or *operator* determines which scenarios require mitigation, when mitigation strategies (protective measures) are implemented to reduce vulnerabilities. The overall desire is to reduce the risk associated with the identified scenario. Note that generally, as mentioned previously, it is easier to reduce vulnerabilities than to reduce consequences or threats when considering mitigation strategies.

To assist the vessel owner and/or *operator* in evaluating the effectiveness of specific mitigation strategies (protective measures), the vessel owner and/or *operator* may find it beneficial to use Table 6 provided below.

Table 6

MITIGATION IMPLEMENTATION WORKSHEET						
1	2	3	4			5
Mitigation Strategy (Protective Measure)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Score (remains the same)**	**New Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility	**+ Organic Security**	**= Total Score**	
1.	1.					
	2.					
	...					
2.	...					

The following steps correspond to each column in Table 6.

1. The vessel owner and/or *operator* should brainstorm mitigation strategies (protective measures) and record them in the first column of Table 6.

2. Using the scenario(s) from Table 5, list all of the scenario(s) that would be affected by the selected mitigation strategy.

3. The consequence score remains the same as was recorded in Table 5 for each scenario.

4. Re-evaluate the vulnerability score (Table 3) for each element, taking into consideration the mitigation strategy, for each scenario.

5. With the consequence score and new total vulnerability score, use Table 4 to determine the new mitigation results.

There are two factors, effectiveness and feasibility, to consider in determining if a mitigation strategy should be implemented. A strategy may be thought of as highly effective if its implementation lowers the mitigation category (e.g. from "mitigate" to

"consider" in Table 4). A strategy may be thought of as partially effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, if a mitigation strategy lowers the vulnerability score from "5-6" to "3-4" while the consequence score remains at "3" and the mitigation category stays at "mitigate."

It should be noted that if a mitigation strategy, when considered individually, does not reduce the vulnerability, that multiple strategies may be considered in combination. Considering mitigation strategies as a whole may allow the vulnerability to be reduced.

A strategy may be thought of as feasible if it can be implemented with little operational impact or funding relative to the prospective reduction in vulnerability. A strategy may be thought of as partially feasible if its implementation requires significant changes or funding relative to the prospective reduction in vulnerability. A strategy may be thought of as not feasible if its implementation is extremely problematic or is cost prohibitive.

The vessel owner and/or *operator* should keep in mind that some strategies may be deployed commensurate with various security threat levels established. Feasibility of a mitigation strategy may vary based on the *MARSEC level*, therefore some strategies may not be warranted at *MARSEC Level 1*, but may be at *MARSEC Levels 2* or 3. For example, using divers to inspect the underwater pier structures and vessel may not be necessary at *MARSEC Level I*, but may be necessary if there is a specific threat and/or an increase in *MARSEC level*. Mitigation strategies should ultimately ensure that a level of security is maintained to achieve the objectives discussed in enclosure (1).

As an example of a possible vulnerability mitigation measure, a company may implement security patrols by hiring additional personnel to detect and prevent unauthorized persons from entering spaces below the main deck on a passenger ferry. This measure would improve organic security and may reduce the overall vulnerability score from a "high" to a "medium". This option, however, is specific for this scenario and also carries a certain cost. Another option might be to secure all access points to spaces below the main deck. This may reduce the accessibility score from "high" to "medium". This option does not require additional personnel and is a passive mitigation measure. Similarly, other scenarios can be tested to determine the most effective strategies.

The vessel owner and/or *operator* should develop a process through which overall security is continually evaluated by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied.

Appendix C

Vessel Security Plan Outline

This section provides a recommended outline of a Vessel Security Plan. In developing this plan, a vessel will be able to address physical security, the protective measures to be taken at each MARSEC level, and how procedures and protective measures are to be implemented.

1. Introduction
   1.1. Purpose & Objectives

2. Vessel Details
   2.1. Vessel Physical Characteristics

3. Company Security Officer
   3.1. Designation
   3.2. Duties and Responsibilities

4. *Vessel Security Officer*
   4.1. Designation
   4.2. Duties and Responsibilities
   4.3. Liaison with Waterfront Facility Security Officers

5. Plan Documentation
   5.1. Periodic Review Procedures
   5.2. Plan Security and Control

6. Communication and Coordination with
   6.1. Port
   6.2. Waterfront facility
   6.3. Law Enforcement
   6.4. Company, the CSO, and the VSO

7. Vessel Security Assessment

8. Maritime Security (MARSEC) Levels and Associated Measures
   8.1. MARSEC Levels
   8.2. MARSEC Level 1
   8.3. MARSEC Level 2
   8.4. MARSEC Level 3

9. Security Actions

10. Ensuring the performance of all vessel security duties

10.1. Duties and responsibilities of watchstanders
10.2. Communication
10.3. Briefings

11. Monitoring *restricted areas* to ensure that only authorized persons have access
11.1. Establishment of *Restricted Areas*
11.2. Methods to Monitor and/or Restrict Access
11.3. Intrusion Detection Devices

12. Controlling access to the vessel
12.1. Access control measures

13. Monitoring of deck areas and areas surrounding the vessel
13.1. Methods
13.2. Security patrol, Procedures
13.3. Surveillance
13.4. Communication Procedures
13.5. Lighting

14. Controlling the embarkation of persons and their effects
14.1. Identification and Visitor Control System
14.2. Screening Procedures

15. Supervising the handling of cargo and vessel's stores
15.1. Screening Procedures

16. Ensuring that port-specific security communication is readily available
16.1. Communication Procedures

17. Vessel/Waterfront Facility Interface
17.1. Procedure for interfacing with Port Facilities

18. Training and Drills
18.1. Procedures for training and exercises and drills associated with the plan

19. Contingency Plans & Standard Operating Procedures (SOP's)
Such as:
19.1. Bomb Threat on vessel
19.2. Bomb Threat to waterfront facility where vessel is moored
19.3. Evacuation of the vessel
19.4. Security Procedures while in drydock or extended maintenance
19.5. Response to Breach of Security or to Suspicious Activity on, or near, the vessel, including provisions for maintaining critical operations of the vessel.

Appendix D

Declaration of Security

_____ (Name of Vessel)

_____ (Name of Waterfront facility)

This *Declaration of Security* is valid from _____ until _____, for the following *vessel/waterfront facility interface* activities under Security Level ____:

The vessel and waterfront facility agree to the following security responsibilities.

Activity	(Initial blank or circle responsible party) **Vessel**	**Facility**
1. Communications established between the vessel and waterfront facility:	_____	_____
a. Means of raising alarm agreed between vessel and waterfront facility.	_____	_____
b. Vessel/waterfront facility report/communicate any noted security non-conformities and notify appropriate government agencies.	_____	_____
c. Port specific security information passed to vessel and notification procedures established (Specifically who contacts local authorities, National Response Center, and Coast Guard).	_____	_____
2. Responsibility for checking identification and screening of:		
a. Passengers, crew, hand carried items, and luggage.	**Vessel / Facility**	
b. Vessel store's, cargo, and vehicles.	**Vessel / Facility**	
3. Responsibility for searching the berth/pier directly surrounding the vessel.	**Vessel / Facility**	
4. Responsibility for monitoring and/or performing security of water surrounding the vessel.	**Vessel / Facility**	
5 Verification of increased MARSEC level and implementation of additional protective measures.	_____	_____
6. Establish protocol to coordinate response between Vessel/Waterfront facility to acts that threaten either the Vessel and/or Waterfront facility	_____	_____

The signatories to this agreement certify that security arrangements for both the vessel and the waterfront facility during the specified *vessel/waterfront facility interface* activities are in place and maintained.

Date of issue .....

_____
(Signature of Master or *Vessel Security Officer*)

_____
Name and Title, *Vessel Security Officer*
Contact information_____

_____
IMO number:

_____
(Signature of Facility Security Officer or authorized designee)

_____
Name and Title, Facility Security Officer
Contact information_____

_____
Mailing address: